CLAIMS

I claim:

1. A method for impersonating, comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity;

authenticating said first entity based on said authentication credentials for said first entity;

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully; and

authorizing said first entity to access a first resource as said second entity based on said cookie.

2. A method according to claim 1, further comprising the step of:

providing a form for said authentication credentials, said form includes a request for a user identification, a password and an impersonatee identification, said user identification and said password correspond to said authentication credentials for said first entity, said impersonatee identification corresponds to said identification of said second entity.

3. A method according to claim 1, wherein:

said step of receiving is performed by an access system;

said access system protects said first resource; and

said first resource is separate from said access system.

4. A method according to claim 1, wherein:

said step of receiving is performed by an access system;

said access system protects a plurality of resources; and

said plurality of resources includes said first resource.

5. A method according to claim 1, wherein:

said cookie stores a distinguished name of said second entity and an IP address for said first entity.

6. A method accord to claim 1, further comprising the steps of:

receiving a request to access said first resource;

providing a form for said authentication credentials, said form includes a request for a user identification, a password and an impersonatee identification, said user identification and said password correspond to said authentication credentials for said first entity, said impersonatee identification corresponds to said identification of said second entity; and

transmitting said cookie for storage on a device being used by said first entity to send said request to access said first resource.

7. A method according to claim 1, wherein:

said steps of receiving, authenticating and authorizing are performed by an access system;

said access system provides access management services and identity management services; and

said first resource is protected by, but separate from, said access system.

8. A method according to claim 1, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity profile.

9. A method according to claim 8, wherein:

said steps of searching a directory server for a first user identity profile and verifying said password based on said user identity profile are performed by a first authentication plug-in; and

said steps of searching said directory server for a second user identity profile and accessing one or more attributes of said second user identity profile are performed by a second authentication plug-in.

10. A method according to claim 1, wherein:

said cookie stores a distinguished name for said second entity; and

said step of authorizing includes the steps of:

accessing said distinguished name stored in said cookie,

accessing a user identity profile for said second entity based on said distinguished name,

accessing a set of one or more authorization rules for said first resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said first resource.

11. A method according to claim 1, wherein:

said authentication credentials correspond to a set of attributes for said first entity;

said identification of said second entity corresponds to a set of attributes for said second entity;

said step of authorizing is based on one or more of said attributes for said first entity; and

said step of authorizing is based on one or more of said attributes for said second entity.

12. A method according to claim 1, wherein:

said authentication credentials correspond to a set of attributes for said first entity; and

said step of authorizing is not based on attributes for said first entity.

13. A method according to claim 1, further comprising the steps of:

receiving a request for a login form; and

providing said login form, said login form includes a request for a user identification, a password and an impersonatee identification, said user identification and said password correspond to said authentication credentials for said first entity, said impersonatee identification corresponds to said identification of said second entity.

14. A method according to claim 1, further comprising the steps of:

receiving a request from said first entity to access a second resource after said step of creating said cookie;

accessing contents of said cookie and determining not to authenticate said first entity in response to said request to access said second resource; and

authorizing said first entity to access said second resource as said second entity based on said cookie, said step of authorizing said first entity to access said second resource is performed without authenticating said first entity in response to said request to access said second resource.

15. A method according to claim 1, wherein:

said steps of authenticating and authorizing are performed without knowing a password for said second entity.

16. A method for impersonating, comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a first resource that is separate from said access system;

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system; and

authorizing said first entity to access said first resource as said second entity, said step of authorizing is performed by said access system.

17. A method according to claim 16, wherein:

said steps of authenticating and authorizing are performed without knowing a password for said second entity.

18. A method according to claim 16, wherein:

said access system protects a plurality of resources that are separate from said access system; and

said plurality of resources includes said first resource.

19. A method according to claim 16, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity profile.

20. A method according to claim 16, wherein:

said steps of searching a directory server for a first user identity profile and verifying said password based on said user identity profile are performed by a first authentication plug-in; and

said steps of searching said directory server for a second user identity profile and accessing one or more attributes of said second user identity profile are performed by a second authentication plug-in.

21. A method according to claim 16, wherein:

said step of authenticating provides a name for said second entity; and

said step of authorizing includes the steps of:

accessing said name,

accessing a user identity profile for said second entity based on said name,

accessing a set of one or more authorization rules for said resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said resource.

22. A method according to claim 16, wherein:

said authentication credentials correspond to a set of attributes for said first entity;

said identification of said second entity corresponds to a set of attributes for said second entity;

said step of authorizing is based on one or more of said attributes for said first entity; and

said step of authorizing is based on one or more of said attributes for said second entity.

23. A method according to claim 16, further comprising the steps of:

receiving a request to access a second resource from said first entity after said step of authenticating said first entity, said access system protects said second resource; and

authorizing said first entity to access said second resource as said second entity, said step of authorizing said first entity to access said second resource is performed without authenticating said first entity in response to said request to access said second resource.

24. A method for impersonating, comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a plurality of resources;

receiving an indication of one or more of said plurality of resources;

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system; and

authorizing said first entity to access said one or more of said plurality of resources as said second user, said step of authorizing is performed by said access system.

25. A method according to claim 24, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity profile.

26. A method according to claim 24, wherein:

said step of authenticating provides a name for said second entity; and

said step of authorizing includes the steps of:

accessing said name,

accessing a user identity profile for said second entity based on said name,

accessing a set of one or more authorization rules for said resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules.

27. A method according to claim 24, wherein:

said authentication credentials correspond to a set of attributes for said first entity;

said identification of said second entity corresponds to a set of attributes for said second entity;

said step of authorizing is based on one or more attributes for said first entity; and

said step of authorizing is not based on attributes for said first entity.

28. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity;

authenticating said first entity based on said authentication credentials for said first entity;

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully; and

authorizing said first entity to access a first resource as said second entity based on said cookie.

29. One or more processor readable storage devices according to claim 28, wherein:

said steps of receiving, authenticating and authorizing are performed by an access system;

said access system protects a plurality of resources separate from said access system; and

said plurality of resources includes said first resource.

30. One or more processor readable storage devices according to claim 28, wherein:

said cookie stores a distinguished name of said second entity and an IP address for said first entity.

31. One or more processor readable storage devices according to claim 28, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity profile.

32. One or more processor readable storage devices according to claim 28, wherein:

said cookie stores a distinguished name for said second entity; and

said step of authorizing includes the steps of:

accessing said distinguished name stored in said cookie,

accessing a user identity profile for said second entity based on said distinguished name,

accessing a set of one or more authorization rules for said first resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said first resource.

33. One or more processor readable storage devices according to claim 28, wherein:

said authentication credentials correspond to a set of attributes for said first entity;

said identification of said second entity corresponds to a set of attributes for said second entity;

said step of authorizing is based on one or more of said attributes for said first entity; and

said step of authorizing is based on one or more of said attributes for said second entity.

34. One or more processor readable storage devices according to claim 28, wherein:

receiving a request from said first entity to access a second resource after said step of creating said cookie;

accessing contents of said cookie and determining not to authenticate said first entity in response to said request to access said second resource; and

authorizing said first entity to access said second resource as said second entity based on said cookie, said step of authorizing said first entity to access said

second resource is performed without authenticating said first entity in response to said request to access said second resource.

35. An apparatus for providing access management that allows for impersonating, comprising:

a communication interface;

a storage device; and

a processing unit in communication with said communication interface and said storage device, said processing unit performs a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity,

authenticating said first entity based on said authentication credentials for said first entity,

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully, and

authorizing said first entity to access a first resource as said second entity based on said cookie.

36. An apparatus according to claim 35, wherein:

said steps of receiving, authenticating and authorizing are performed by an access system;

said access system protects a plurality of resources separate from said access system; and

said plurality of resources includes said first resource.

37. An apparatus according to claim 35, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity profile.

38. An apparatus according to claim 35, wherein:

said cookie stores a distinguished name for said second entity; and

said step of authorizing includes the steps of:

accessing said distinguished name stored in said cookie,

accessing a user identity profile for said second entity based on said distinguished name,

accessing a set of one or more authorization rules for said first resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said first resource.

39. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a first resource that is separate from said access system;

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system; and

authorizing said first entity to access said first resource as said second entity, said step of authorizing is performed by said access system.

40. One or more processor readable storage devices according to claim 39, wherein:

said access system protects a plurality of resources that are separate from said access system; and

said plurality of resources includes said first resource.

41. One or more processor readable storage devices according to claim 39, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity profile.

42. One or more processor readable storage devices according to claim 39, wherein:

said step of authenticating provides a name for said second entity; and

said step of authorizing includes the steps of:

accessing said name,

accessing a user identity profile for said second entity based on said name,

accessing a set of one or more authorization rules for said resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said resource.

43. One or more processor readable storage devices according to claim 39, wherein:

said authentication credentials correspond to a set of attributes for said first entity;

said identification of said second entity corresponds to a set of attributes for said second entity;

said step of authorizing is based on one or more of said attributes for said first entity; and

said step of authorizing is based on one or more of said attributes for said second entity.

44. One or more processor readable storage devices according to claim 39, wherein said method further comprises the steps of:

receiving a request to access a second resource from said first entity after said step of authenticating said first entity, said access system protects said second resource; and

authorizing said first entity to access said second resource as said second entity, said step of authorizing said first entity to access said second resource is performed without authenticating said first entity in response to said request to access said second resource.

45. An apparatus for providing access management that allows for impersonating, comprising:

a communication interface;

a storage device; and

a processing unit in communication with said communication interface and said storage device, said processing unit performs a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a first resource that is separate from said access system,

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system, and

authorizing said first entity to access said first resource as said second entity, said step of authorizing is performed by said access system.

46. An apparatus according to claim 45, wherein:

said access system protects a plurality of resources that are separate from said access system; and

said plurality of resources includes said first resource.

47. An apparatus according to claim 45, wherein:

said authentication credentials include an ID and a password;

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said identification of said second entity, and

accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity profile.

48. An apparatus according to claim 45, wherein:

said step of authenticating provides a name for said second entity; and

said step of authorizing includes the steps of:

accessing said name,

accessing a user identity profile for said second entity based on said name,

accessing a set of one or more authorization rules for said resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said resource.